Tipos de ataques. Cómo actúan los hackers.

Definición:

Un ataque informático es un intento intencionado y organizado para infringir daños o problemas en un sistema informático o red. Estos ataques suelen estar causados por una o varias personas. Estas personas que producen estos ataques informáticos están organizados en grupos llamados “piratas informáticos”.

Causa de ataques informáticos:

Un ataque se produce por un fallo o debilidad en el software, hardware o personas que forman parte de un ambiente informático. Esto causa un efecto negativo en el sistema y también produce efecto negativo en los activos de la organización.

Los ataques suelen ser a organizaciones.

Diferencias entre hacker, pirata informático y cracker:

Hacker: Se trata de aquella persona que posee conocimientos en tecnología informática, ellos hacen entradas remotas no autorizadas desde una red de comunicaciones a sistemas para probar su vulnerabilidad y poder corregir sus debilidades. También se llama así a un grupo de programadores y diseñadores de sistemas entusiastas pertenecientes al MIT en los años 60. Estos últimos impulsaron el lanzamiento del software libre.

Pirata informático: Este grupo de personas se dedica a la apropiación, reproducción, acaparación y distribución de software de terceros, con fines lucrativos, a gran escala, y sin aportar ninguna mejora.

Crackers: Son aquellos que se dedican a atacar los sistemas desde una perspectiva de causar daños, alterar la información o con finalidad destructiva.

Tipos de hacker:

Hackers de sombrero blanco: Son los hackers descritos antes que rompen la seguridad del sistema de empresas y compañías para mejorar su seguridad, estos suelen trabajar en el departamento de seguridad informática de empresas y compañías.

Hackers de sombrero negro: Son aquellas personas que se describen con la definición de crackers. Estas personas atacan los sistemas informáticos con el fin de hacer daño a empresas y organizaciones y/o robar información produciendo efectos negativos en personas, empresas o organizaciones.

Hackers de sombrero gris: Son aquellas personas que hacen los mismos daños que los hackers de sombrero negro pero luego cobran a las empresas, organizaciones o personas por reparar los daños que han causado.

Tipos de ataques:

Existen dos tipos de ataques.
Ataques pasivos: Intenta hacer uso o aprender de la información del sistema, no afecta a los recursos del sistema.
Ataques activos: Intentan alterar los recursos del sistema o alterar su funcionamiento.

En los ataques pasivos tenemos los siguientes ataques y cómo actúan las personas que producen estos ataques:

-wiretapping: Es la monitorización de conversaciones telefónicas y de internet por parte de terceros, producida con frecuencia por organizaciones encubiertas. Las escuchas ilegales a través de internet se producen usando herramientas como Aircrack-ng o Kismet. Una vez dentro del sistema el hacker utilizará ataques como spoofing ARP para ver los paquetes que le interesan utilizando herramientas como wireshark o ettercap. También se envía al usuario un archivo mp3 o una imagen que contiene el archivo que producirá el ataque wiretapping.

Para las grabaciones mediante teléfonos móviles se utiliza un dispositivo llamado IMSI-catcher. Este ataque se hace a la comunicación entre el teléfono y la red con un ataque Man-in-the-middle. Esto es posible porque el teléfono se tiene que autentificar con la red de telefonía y la red no mande la autentificación. Estos ataques no se pueden evitar, excepto con el cifrado end-to-end que se están incluyendo en los nuevos teléfonos.

-Port scan: Este ataque consiste en enviar un mensaje a cada puerto de un dispositivo conectado a la red y ver cual devuelve una respuesta, este puerto será utilizado para los ataques de los hackers.

Se utiliza la técnica scan stealth que consiste en hacer un escaneo en un puerto muy lentamente para pasar desapercibido por las herramientas de detección.

SOCKS port probe : Este sistema SOCKS permite que varias máquinas se conecten a la misma conexión de internet. Los atacantes utilizan este puerto porque les permite controlar las máquinas fuentes y destinos y utilicen esto para utilizar nuestro ordenador para ocultar su verdadera ubicación.

Bounce scan: Los atacantes buscan en internet sistemas a los que puedan rebotar sus ataques.

UDP scanning: Estos puertos los utilizan los atacantes para ver que puertos pueden utilizar. Es fácil bloquearlos.

-Idle scan: Método que consiste en enviar paquetes falsos a un ordenador para ver qué servicios están activos. Esto se consigue mediante la suplantación de una computadora llamada “zombie” y observando el comportamientos de la computadora “zombie”.

En los ataques activos tenemos los siguientes ataques.

-Denial-of-service attack(DoS): Es un ataque informático donde el atacador pretende que una máquina o recurso de red no esté disponible para los usuarios que van a utilizarlo. Esto se consigue llenando la máquina con peticiones superfluas sobrecargando el sistema que se está atacando para que evitar que se ejecute las peticiones importantes hechas por el usuario autorizado a utilizar la máquina o recurso web.

Los ataques Denial-of-service-distributed es lo mismo que el ataque denial-of-service pero producido desde diferentes máquinas, haciendo más difícil detener el ataque.

-Spoofing attack: Es un ataque que se produce porque una persona ha conseguido suplantar una identidad con éxito para obtener una ventaja de ilegitimidad.

Spoofing TCP/IP: Los paquetes de protocolo TCP/IP no tienen mecanismos de detección de origen y destino de los mensajes recibidos por lo que son susceptibles de sufrir spoofing attacks. La suplantación de IP y la de ARP se suele utilizar para hacer ataques man-in-the-middle contra máquinas hosts en una red de ordenadores. Estos ataques se pueden prevenir con firewalls que hagan una búsqueda exhaustiva de paquetes o verificando identidad del remitente y destinatario.

Referrer-Spoofing: Algunas páginas de pago permiten acceder a su información a través de un acceso identificado donde se hace una comprobación del encabezado HTTP el cual puede ser suplantado, permitiendo a los usuarios tener acceso no autorizado a los contenidos de la página.

Poisoning of file-sharing networks: Son los ataque que producen que haya obras distorsionadas o inservibles en una red de intercambio de archivos infringiendo los derechos de autor de los autores de la obra.

Caller ID spoofing: Este ataque produce la falsificación de nombres y números en las redes de telefonía pública donde se hace una llamada a una persona y la parte que hace la llamada falsifica el nombre y número de la persona a la que ha llamado.

E-mail address spoofing: Este ataque produce que los spammers puedan ocultar sus correos electrónicos. También produce suplantación de las direcciones de correo electrónico, estas se producen como en el correo convencional. Donde el protocolo SMTP envía un mensaje, esto se puede hacer con un servidor de correo telnet.

GPS spoofing: Este ataque consiste en falsificar los datos de la señal GPS, para ello la persona que produce este ataque envía señales sincronizadas con las señales genuinas

aumentando la potencia de las señales falsificadas gradualmente hasta que se aleja de las señales genuinas.

-Man-in-the-middle: Este ataque produce que dos partes que creen que se comunican entre sí se está alterando la comunicación entre sí o la están transmitiendo. El atacante tiene que emitir mensajes a las dos partes, y también controla toda la comunicación entre las dos partes.

-ARP poisoning: El atacante envía mensajes de resolución de dirección de protocolo a una red de área local, con el objetivo de asociar la dirección MAC del atacante con la dirección IP de la máquina host haciendo que el tráfico que se envíe a esa IP se le envía al atacante en su lugar.

-Ping flood: Este ataque se basa en enviar muchos paquetes ping ICMP lo más rápido posible sin esperar respuesta de la máquina destino. El atacante espera que se responda con paquetes de respuesta eco ICMP consumiendo así el ancho de banda de salida y el ancho de banda de entrada, si la máquina de destino es suficiente lenta es posible consumir ciclos de CPU para que se note una reducción del rendimiento.

-Ping of death: Cuando se mandan paquetes ping a una máquina estos paquetes pueden tener tamaño de 56 bytes o 64 bytes, pero cualquier paquete mandado bajo el protocolo IPv4 puede tener como mucho un tamaño de 65535 bytes. Como muchos sistemas informáticos no han sido diseñados para un paquete ping de tamaño tan grande el ping de la muerte lo que hace es mandar paquetes ping de tamaño 65535. Como los paquetes ping se dividen en bloques de 8 bytes cuando son mandados después en la máquina destino tienen que volver a unir esto paquetes. Cuando la máquina destino monta los paquetes divididos de un paquete que mide 65535 bytes, produce desbordamiento del buffer provocando fallos del sistema y permitiendo alojar código malicioso en la máquina de destino.

-Smurf attack: En este ataque el atacante falsifica una dirección IP que será la dirección de la víctima, envía paquetes ICMP utilizando la dirección IP falsificada a todas las máquinas de una red, cuando las máquinas responden enviando la respuesta a la dirección IP utilizada por el atacante, esto hace que se sobrecargue la máquina de la dirección de la víctima hasta el punto donde se le hace imposible trabajar a la víctima en su máquina.

-Buffer overflow: En este ataque el atacante sobreescribe memoria adyacente a un buffer que no debería haber sido modificada. El atacante utiliza esto para cambiar valores importantes de la pila de llamadas al sistema, con el fin de ejecutar su código sin que se detecte como malicioso.

-Heap overflow: Este ataque es un tipo de ataque buffer overflow, que está dirigido específicamente al heap. En los ataques al heap se sobreescriben datos de la pila para explotar algún aspecto del programa. Un ataque al heap corrompen la información para cambiar cosas que los atacantes quieren cambiar. En estos ataques se pueden

sobreescribir los datos del heap, o se puede sobreescribir un puntero para que apunte a un punto de código malicioso del atacante.

-Format string attack: Este ataque se produce cuando los datos enviados a través de una cadena de entrada se evalúan como comandos. El atacante puede ejecutar su propio código, leer la pila o causar algún error de segmentación, el cual provocaría nuevos comportamientos y podría comprometer la seguridad y la estabilidad de la máquina a la que va dirigido el ataque.

Enlaces:

https://sites.google.com/site/piratasinformaticosproject/origen-de-los-hackers
https://es.wikipedia.org/wiki/Hacker
https://en.wikipedia.org/wiki/Attack_(computing)#Types_of_attack
https://en.wikipedia.org/wiki/Telephone_tapping
https://answers.yahoo.com/question/index?qid=20061105020422AAtre1p
https://en.wikipedia.org/wiki/Idle_scan
https://en.wikipedia.org/wiki/Denial-of-service_attack
https://en.wikipedia.org/wiki/Spoofing_attack
https://en.wikipedia.org/wiki/Man-in-the-middle_attack
https://en.wikipedia.org/wiki/ARP_spoofing
https://en.wikipedia.org/wiki/Ping_flood
https://en.wikipedia.org/wiki/Ping_of_death
https://en.wikipedia.org/wiki/Smurf_attack
https://www.ibm.com/support/knowledgecenter/SSB2MG_4.6.0/com.ibm.ips.doc/concepts/wap_buffer_overflow.htm
https://security.radware.com/ddos-knowledge-center/ddospedia/buffer-overflow-attack/
https://en.wikipedia.org/wiki/Buffer_overflow
https://sites.google.com/site/bufferattack/attacks/heap
https://es.wikipedia.org/wiki/Format_String_Attack
https://en.wikipedia.org/wiki/Uncontrolled_format_string